Docket No. BOC9-2003-0073 (444)

METHOD AND SYSTEM FOR MANAGING THE DISPLAY OF SENSITIVE CONTENT IN NON-TRUSTED ENVIRONMENTS

Inventor(s):

Tsz Simon Cheng

Brent W. Cossey

Gregory P. Fitzpatrick

International Business Machines Corporation

IBM Docket No. BOC9-2003-0073

IBM Disclosure No. BOC8-2003-0094

Express Mailing Label No. EV 346756854 US

METHOD AND SYSTEM FOR MANAGING THE DISPLAY OF SENSITIVE CONTENT IN NON-TRUSTED ENVIRONMENTS

Technical Field

[0001] This invention relates to the field of data management and more particularly to a method and system of managing sensitive content in non-trusted environments.

Description of the Related Art

[0002] In the current business environment, documents or other objects containing sensitive or confidential content can be viewed on a user's portable computing device in virtually any location. For instance, a user can view confidential corporate documents on his/her machine in a variety of public or "non-trusted" areas such as an airport, airplane, or hotel restaurant. Many employees tend to pay very little attention to their surrounding environment when it comes to confidential documents due to time constraints, or simply lack of attention. As a result, employees from competitive firms are can potentially view material that is intended solely for a given employees' consumption. Additionally, employees of the same firm may inadvertently share confidential information that is not intended for both employees.

[0003] Today, enterprises have few tools to enforce corporate data security policies in these situations. For data that permanently resides both on a portable computing device (like an IBM Thinkpad or a personal Digital Assistant or PDA) as well as data that is delivered to such devices dynamically over a network, companies have no effective methods to prevent or restrict mobile employees from viewing sensitive data in non-trusted environments.

SUMMARY OF THE INVENTION

[0004] Embodiments in accordance with the invention can enable and enforce a corporate-wide security policy regardless of whether an employee is working in a company office ("trusted area") or in some remote location ("non-trusted" area). The service can operate as an extension to existing operating systems, middleware, or end-user applications. It is also possible to extend the function to a system's firmware, enabling restrictions on a device's being used at all (i.e., restrictions on boot-up capability).

[0005] In a first aspect of the invention, a method for managing the display of sensitive content in non-trusted environments can include the steps of interrogating a list of policies associated with a given user and a physical device, determining a location of the physical device, comparing the location of the physical device with a list of trusted locations, and enforcing a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location.

[0006] In a second aspect of the invention, a system for managing the display of sensitive content in non-trusted environments can include a memory, a display, and a processor coupled to the memory and the display. The processor can be programmed to interrogate a list of policies associated with a given user and a physical device, determine a location of the physical device, compare the location of the physical device with a list of trusted locations, and enforce a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location.

[0007] In a third aspect of the invention, a computer program has a plurality of code sections executable by a machine for causing the machine to perform certain steps as described in the method and systems above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] There are shown in the drawings embodiments which are presently preferred, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown.

[0009] FIG. 1 is a flow diagram illustrating a method for managing the display of sensitive content in non-trusted environments in accordance with the present invention.

[0010] FIG. 2 is an exemplary system for managing the display of sensitive content in non-trusted environments in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] Referring to FIG. 1, a method 10 for managing the display of sensitive content in non-trusted environments can include the step 12 of interrogating a list of one or more corporate policies associated with the given user and physical device. (Multiple policies may be complementary, that is, a basic policy may describe general rules, whereas complementary policies describe more details, exception conditions, etc.) Policy data may be instantiated in either clear text or encrypted, using either proprietary formats or industry-standard formats, as they become available. This policy data may be acquired either locally from the device to be managed or dynamically via access to the corporate network - either directly attached to the network or indirectly via the Internet or other service. Each corporate policy may be coarse-grained (e.g., permitting no access to any data in a non-trusted zone) or fine-grained (e.g., permitting no access to specific company-confidential data elements within certain proscribed classes of documents). Upon interrogation of the policy or policies, the invention proceeds to enforce the rules at step 20 contained in the policy.

[0012] In this particular embodiment, before the rules are enforced, the location of the physical device can be determined at step 14. Since the method 10 is primarily intended to operate when the user is physically located in a non-trusted location, awareness of the user's (approximate) location will be crucial in this embodiment. To enable this capability, the service can make use of a positioning technology, such as a GPS (Global Positioning Satellite) system and/or a wireless infrastructure (cellular network or WIFI) which could determine a user's location as indicated at step 16. While GPS is suitable for outdoor environments and could be accessed anywhere globally,

wireless infrastructure is suitable for both indoor and outdoor environments, but is subject to limited availability based on location. A combination of the two technologies for retrieving location information can also be used. Other location technologies may be substituted without deviating from the spirit of this invention.

[0013] The invention would next compare at step 18 the determined location to the organization's list of trusted zones, which may be imbedded within the corporate policy object or elsewhere. (Note that the organization may include a user-specific trusted zone, such as a user's home address.) This embodiment of the invention could then determine whether the user is in a "trusted" or "non-trusted" zone (e.g., corporate office vs. airplane) and prompt the user with the actions dictated by the appropriate corporate policy. As a user moves to new locations, the system can recognize the new location and re-compares locations to the list of trusted zones and enforces the policy at step 20 by restricting or relaxing access to objects or allows the user to continue in the current mode uninterrupted.

[0014] To implement restricted access to this data, the method 10 can, for instance, render on the user's screen a version of the document/object with portions either "blacked out" or simply not accessible in some manner. Techniques for limiting access as indicated in step 22 include (but are not limited to):

a) Blacking-out sensitive data (for text or graphical objects) or including 'white noise' gaps in audio or video objects

b) Replacing sensitive data with innocuous data (e.g., 'Restricted', if a text object)

c) Prohibiting access to the object (i.e., user is aware of its existence, but cannot access it)

d) Hiding the object from the user (i.e., casual user/observer is not even aware of its existence)

[0015] Rules enforcement may take a number of different forms. The preferred embodiment would be one in which, upon detection of a user's attempt to access a document, file or object, the service would prompt the user to remind him/her of the corporate policy regarding confidential material as shown at optional step 24. The service can further challenge the user to provide authentication at step 26. The process of verifying that the person with whom a system is communicating or conducting a transaction is, in fact, that specific individual is referred to as authentication. Authentication is a process that can be accomplished using one of three approaches as indicated by step 28 where either a) unique knowledge (something the individual knows such as a pin number) b) a unique possession (something the individual has such as an access card) or c) a unique characteristic (something physiologically unique about the individual such as a fingerprint, voiceprint, or retinal scan). This method can utilize any combination of these three approaches. For instance, it may verify identity in the form of a password challenge, fingerprint identification, retinal scan or similar biometric technology.

[0016] Having authenticated the individual in question as well as his/her location, the method 10 can utilize a set of keywords and/or object properties/attributes which are deemed to be sensitive or confidential. The description of these keywords or properties may be defined in the corporate policy or may be simply referenced in the policy and

defined elsewhere, for instance in an industry-standard attribute repository. The invention acquires this data by accessing either the policy or the standard repository.

[0017] Next, the method can access the objects that the user may access, prior to providing the user full access to any of those objects. Those objects may already be 'open', for instance in a GUI-based operating system. The method would then apply the specific policy elements, which can take any of several forms. (In each case, the method itself requires access to all possible sensitive objects as well as their internal formats, since the method needs to be aware of the structure of each object in order to parse it, 'understand' its components and take fine-grained action.) Examples of object attributes that may be restricted include (but are not limited to): a) Corporate revenue information b) Customer names c) Company names d) Personnel information

[0018] Referring to FIG. 2, a system 100 for managing the display of sensitive content in non-trusted environments can include a memory 113, a display 119, and a processor 121 coupled to the memory and the display. The memory 113, display 119, and processor 121 can be part of any number of client devices (112, 114, 116, 124) such as laptops and PDAs. The processor 119 can be programmed to interrogate a list of policies 115 associated with a given user and a physical device, determine a location of the physical device, compare the location of the physical device with a list of trusted locations, and enforce a plurality of rules contained in the policy, wherein access to sensitive information is limited or restricted based on the location. The location information 117 can be obtained using any number of location finding schemes including GPS and wireless infrastructure as previously mentioned. The policies can be

stored locally in the client devices or at remote servers 120 or 130 or even at trusted access points 118 or 124 coupled to the servers via a network 110.

[0019] This system 100 also contemplates a public, subscription-based service which employ a list of employee name/ids, machine identification information from multiple organizations. The service would use GPS technology and tables of machine addresses and corresponding users and organizations. For example, the service could use this data to alert a user (who is viewing a confidential document) when someone from a competitive firm was in their proximity. The user could define a profile which would specify which companies are considered competitive and within what proximity to be notified. This proximity and competitive information could also be acquired via access to a corporate policy, rather than from a given user.

[0020] Further, a corporation could provide role-based user capabilities as an enhancement to the basic service. For example, if an employee were to attempt to open a confidential document he/she could be granted the ability to override the policy with a password, thumb print, retinal scan, etc., as described above. The company could set up roles based on job title, band level, years of experience, etc.. For example, all employees below a certain seniority or pay grade level might not be permitted to override a corporate policy. Conversely, employees with higher rank would be permitted to override corporate policy, pending presentment of the proper authentication credentials. This capability would prevent confidential documents from being seen inadvertently, while allowing highly-trusted employees that ability to share otherwise-prohibited information with other employees, business partners, etc.

[0021] In summary, this system can provide several features allowing organizations to restrict access to machines, objects or even sensitive data elements of single objects by utilizing both corporate policies and users' physical location. The policies are applied to persons with differing access capabilities and enforced by utilizing authentication mechanisms.

[0022] It should be understood that the present invention can be realized in hardware, software, or a combination of hardware and software. The present invention can also be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system or other apparatus adapted for carrying out the methods described herein is suited. A typical combination of hardware and software can be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein.

[0023] The present invention also can be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which when loaded in a computer system is able to carry out these methods. Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following: a) conversion to another language, code or notation; b) reproduction in a different material form.

[0024] This invention can be embodied in other forms without departing from the spirit or essential attributes thereof. Accordingly, reference should be made to the following claims, rather than to the foregoing specification, as indicating the scope of the invention.